ON THE TOPOLOGICAL ASPECTS OF ARITHMETIC ELLIPTIC CURVES

KAZUMA MORITA

Abstract. In this short note, we shall construct a certain topological family which contains all elliptic curves over $\mathbb{Q}$ and, as an application, show that this family provides some geometric interpretations of the Hasse-Weil L-function of an elliptic curve over $\mathbb{Q}$ whose Mordell-Weil group is of rank ≤ 1.

1. Introduction

For any elliptic curve E over $\mathbb{Q}$, there exists a rational newform f such that we have $L(E,s) = L(f,s)$ and, in particular, the Fourier expansion of f tells us the eigenvalues of the Frobenius operator acting on the Tate module of the strong Weil curve modulo p. In this paper, we shall deform the Fourier expansion of f with respect to the arguments $\{\theta_p\}_p$ of these eigenvalues and construct a topological family attached to these deformed differential forms. This family contains all elliptic curves over $\mathbb{Q}$ up to isogeny and we expect that we can deduce the arithmetic facts by using the topological methods. Actually, as an application, if E is an elliptic curve over $\mathbb{Q}$ whose Mordell-Weil group is of rank ≤ 1, we will show that this family provides some geometric interpretations of the Hasse-Weil L-function of E.

Acknowledgments. The author would like to thank Professor Masanori Asakura and Iku Nakamura for useful discussions. This research was partially supported by JSPS Grant-in-Aid for Research Activity Start-up.

2. Review of the classical theory

Let $\mathbb{H}$ be the upper half-plane and $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ be the extended upper half-plane which is obtained by adding the cusps $\mathbb{Q} \cup \{\infty\}$. The modular group $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$ acts discontinuously on $\mathbb{H}$ via linear fractional transformations. Let $\Gamma_0(N)$ denote the congruence subgroup

$$\Big\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid c \equiv 0 \pmod{N}\Big\}$$

Date: January 20, 2013.

1991 *Mathematics Subject Classification.* 11F03, 11G05, 11G40.

Key words and phrases. modular forms, elliptic curves, L-functions,

of Γ. The space of cusp forms of weight 2 for $\Gamma_0(N)$ will be denoted by $S_2(N)$. Then, every cusp form $f(z) \in S_2(N)$ $(z \in \mathbb{H})$ has the Fourier expansion

$$f(z) = \sum_{n=1}^{\infty} a_n(f) q^n \qquad (a_n(f) \in \mathbb{C},\ q = e^{2\pi i z}).$$

We say that $f(z)$ is a normalized cusp form if we have $a_1(f) = 1$. On the other hand, the space of cusp forms $S_2(N)$ is equipped with the Hecke operators:

- $T_p : f(z) \mapsto pf(pz) + \frac{1}{p}\sum_{r=0}^{p-1} f(\frac{z+r}{p}) \qquad (p \nmid N\ (p\text{: prime}))$
- $U_p : f(z) \mapsto \frac{1}{p}\sum_{r=0}^{p-1} f(\frac{z+r}{p}) \qquad (p \mid N\ (p\text{: prime})).$

Now, we are concerned with a *rational newform* f: a normalized cusp form of weight 2 which has the rational Fourier expansion, is a simultaneous eigenform for all the Hecke operators and is a newform in the sense of [AL]. Let δ_N denote the character defined by $\delta_N(p) = 1$ if $p \nmid N$ and $= 0$ if $p \mid N$.

Proposition 2.1. *Let $f(z) = \sum_{n=1}^{\infty} a_n(f) q^n$ be a rational newform. Then, the Fourier expansion of $f(z)$ satisfies the following conditions.*

(1) $a_{p^{r+1}}(f) = a_p(f) a_{p^r}(f) - \delta_N(p) p a_{p^{r-1}}(f) \qquad (r \geq 1)$
(2) $a_{mn}(f) = a_m(f) a_n(f) \qquad ((m, n) = 1).$

Given a rational newform f, we consider an associated period lattice

$$\Lambda_f = \{ \int_{\alpha}^{\beta} f(z) dz \mid \alpha,\ \beta \in \mathbb{H}^*,\ \alpha \equiv \beta \pmod{\Gamma_0(N)} \}$$

which is a discrete subgroup of $\mathbb{C}$ of rank 2. Then, it is known that the quotient $E_f = \mathbb{C}/\Lambda_f$ is an elliptic curve over $\mathbb{Q}$ of conductor N and that we have $L(E_f, s) = L(f, s)$ where the LHS denotes the Hasse-Weil L-function of E_f and the RHS denotes the Dirichlet L-series of f. Conversely, for any elliptic curve E over $\mathbb{Q}$, there exists a rational newform f such that we have $L(E, s) = L(f, s)$ ([Wi], [TW], [BCDT]). From this equality, we have the following result.

Proposition 2.2. *For any prime $p \nmid N$, we have $a_p(f) = 1 + p - \#E_f(\mathbb{F}_p)$ and there exists $0 \leq \theta_p \leq \pi$ such that $a_p(f) = 2p^{\frac{1}{2}} \cos(\theta_p)$.*

3. Deformation of the Fourier expansion

In this section, we shall deform the Fourier expansion of a rational newform with respect to the arguments $\{\theta_p\}_p$ (Proposition 2.2).

Definition 3.1. Let $F(z) = \sum_{n=1}^{\infty} a_n(F) q^n$ be a formal power series in $\mathbb{C}[[q]]$ which satisfies the following conditions.

(1) If there exists a rational newform $f(z)$ such that we have $a_p(f) = a_p(F)$ for almost all primes p, put $F(z) = f(z)$. The coefficients of $F(z)$ are determined by Proposition 2.1 and 2.2.

(2) If there does not exist such a rational newform, assume that $F(z)$ is normalized (i.e. $a_1(F) = 1$) and that, for each prime p, there exists $0 \leq \theta_p^F \leq \pi$ such that we have

$$a_p(F) = 2p^{\frac{1}{2}}\cos(\theta_p^F).$$

Furthermore, the following compatible conditions are satisfied.

(a) $a_{p^{r+1}}(F) = a_p(F)a_{p^r}(F) - pa_{p^{r-1}}(F) \qquad (r \geq 1)$

(b) $a_{mn}(F) = a_m(F)a_n(F) \qquad ((m,n) = 1)$.

Fix a power series $F(z) \in \mathbb{C}[[q]]$ as above. Let $\{\gamma_i\}_{i=1,2}$ denote any smooth path from α_i to β_i in $\mathbb{H}^*$. Consider an associated period lattice

$$\Lambda_F(\gamma_1, \gamma_2) = \{ \int_{\alpha_i}^{\beta_i} F(z)dz \mid \alpha_i \overset{\gamma_i}{\rightsquigarrow} \beta_i \}_{i=1,2}.$$

Note that, contrary to Λ_f, this $\Lambda_F(\gamma_1, \gamma_2)$ does not form a discrete subgroup of $\mathbb{C}$ depending on the choice of $\{\gamma_i\}_{i=1,2}$. Thus, the quotient $E_F(\gamma_1, \gamma_2) = \mathbb{C}/\Lambda_F(\gamma_1, \gamma_2)$ is not an elliptic curve in general.

Definition 3.2. With notation as above, let Θ denote the topological family $\{E_F(\gamma_1, \gamma_2)\}$ where F (resp. $\{\gamma_i\}_{i=1,2}$) runs through any power series as in Definition 3.1 (resp. any smooth path in $\mathbb{H}^*$).

Remark 3.3. We can say that this topological family Θ is the smallest in the sense that it contains all elliptic curves over $\mathbb{Q}$ up to isogeny and the associated rational newforms are all parametrized by the arguments $\{\theta_p\}_p$.

4. Applications

4.1. **The case of rank** 0. For any elliptic curve E over $\mathbb{Q}$, the Birch and Swinnerton-Dyer conjecture predicts that the rank of Mordell-Weil group $E(\mathbb{Q})$ is equal to the order of the zero of $L(E, s)$ at $s = 1$. In the case that we have $L(E, 1) \neq 0$, it is known that the Mordell-Weil group of E is of rank 0 ([CW]). Now, assume that E is such an elliptic curve and that f is an associated rational newform satisfying $L(E, s) = L(f, s)$. Since the Dirichlet L-series $L(f, s)$ can be written via Mellin transform

$$L(f, s) = (2\pi)^s \Gamma(s)^{-1} \int_0^{i\infty} (-iz)^s f(z) \frac{dz}{z}$$

where $\Gamma(s)$ denotes the gamma function of s, the period integral $\int_0^{i\infty} f(z)dz$ does not vanish. Let I denote any smooth path from 0 to $i\infty$ in $\mathbb{H}^*$.

Example 4.1. Let $\{E_i\}_{i=1,2}$ be two elliptic curves over $\mathbb{Q}$. Assume that there exist a set of formal power series $\{F(z)\}_F$ as in Definition 3.1 and a set of smooth paths $\{J\}_J$ in $\mathbb{H}^*$ such that $\{E_F(I, J)\}_{F,J}$ forms a topological family of (non-degenerate) elliptic curves connecting E_1 and E_2. Then, Mordell-Weil groups of $\{E_i\}_{i=1,2}$ are of rank 0.

4.2. **The case of rank 1.** First, we shall recall the results of [GZ]. Let K be an imaginary quadratic field whose discriminant D is relatively prime to the level N of the rational newform f and let H denote the Hilbert class field of K. Fix an element σ in $\mathrm{Gal}(H/K)$. Note that this Galois group is isomorphic to the class group Cl_K of K. Let $\mathcal{A}_K$ be the class corresponding to σ and let $\theta_{\mathcal{A}_K}(z)$ denote the theta series

$$\theta_{\mathcal{A}_K}(z) = \sum_{n \geq 0} r_{\mathcal{A}_K}(n) q^n \quad (q = e^{2\pi i z})$$

where $r_{\mathcal{A}_K}(0) = \frac{1}{\sharp(\mathcal{O}_K^*)}$ ($\mathcal{O}_K$: the ring of integers in K) and $r_{\mathcal{A}_K}(n)$ ($n \geq 1$) is the number of integral ideals α in the class of $\mathcal{A}_K$ with norm n. Define the L-function associated to the rational newform $f = \sum_n a_n q^n \in S_2(N)$ and the ideal class $\mathcal{A}_K$ by

$$L_{\mathcal{A}_K}(f, s) = \left(\sum_{n \geq 1, (n, DN)=1} \epsilon_K(n) n^{1-2s} \right) \cdot \left(\sum_{n \geq 1} a_n r_{\mathcal{A}_K}(n) n^{-s} \right)$$

where $\epsilon_K : (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$ denotes the character associated to $K/\mathbb{Q}$. Furthermore, for a complex character χ of the ideal class group of K, denote the total L-function by

$$L(f, \chi, s) = \sum_{\mathcal{A}_K} \chi(\mathcal{A}_K) L_{\mathcal{A}_K}(f, s).$$

Then, it is known that both of $L_{\mathcal{A}_K}(f, s)$ and $L(f, \chi, s)$ have analytic continuations to the entire plane and satisfy functional equations ($s \leftrightarrow 2 - s$). Furthermore, if we put $L_{\epsilon_K}(f, s) = \sum_n \epsilon_K(n) a_n n^{-s}$ for $f = \sum_n a_n q^n$, we have $L(f, s) L_{\epsilon_K}(f, s) = L(f, \mathbf{1}, s)$. Note that $L_{\epsilon_K}(f, s)$ is the Hasse-Weil L-function of E' over $\mathbb{Q}$ where E' denotes the twist of E over K ([GZ, p.309, 312]). The following thing is one of the main results of Gross-Zagier.

Proposition 4.2. *([GZ, p.230]) There exists a cusp form $g_{\mathcal{A}_K}$ of weight 2 on $\Gamma_0(N)$ such that we have*

$$L'_{\mathcal{A}_K}(f, 1) = 32\pi^2 \sharp(\mathcal{O}_K^*)^{-2} |D|^{-\frac{1}{2}} \cdot (g_{\mathcal{A}_K}, f)_N$$

where $(\ ,\ )_N$ denotes the Petersson inner product on cusp forms of weight 2 for $\Gamma_0(N)$. Thus, this formula leads to

$$L'(f, \chi, 1) = \sum_{\mathcal{A}_K} \chi(\mathcal{A}_K) L'_{\mathcal{A}_K}(f, 1) = 32\pi^2 \sharp(\mathcal{O}_K^*)^{-2} |D|^{-\frac{1}{2}} \cdot (\sum_{\mathcal{A}_K} \chi(\mathcal{A}_K) g_{\mathcal{A}_K}, f)_N$$

Now, let E be an elliptic curve over $\mathbb{Q}$ such that $L(E, s) = L(f, s)$ for some rational newform $f \in S_2(N)$. Assume that we have $\mathrm{ord}_{s=1} L(E, s) = 1$. In this case, it is known that the Mordell-Weil group of E is of rank 1 ([Ko]). Furthermore, since the sign of the functional equation of $L(E, s) = L(f, s)$ is -1, we can choose an imaginary quadratic extension $K/\mathbb{Q}$ such that $L_{\epsilon_K}(f, 1) \neq 0$ ([Wa]). In particular, it follows that we obtain $L'(f, \mathbf{1}, 1) \neq 0$ and thus $(\sum_{\mathcal{A}_K} \mathbf{1}(\mathcal{A}_K) g_{\mathcal{A}_K}, f)_N \neq 0$.

Let $\{g_i\}_{i=1}^d$ (resp. $\{h_j\}_{j=1}^e$) denote a basis of the space of newforms (resp. oldforms) in $S_2(N)$ over $\mathbb{C}$. If we write $\sum_{\mathcal{A}_K} \mathbf{1}(\mathcal{A}_K) g_{\mathcal{A}_K} = \sum_{i=1}^d a_i g_i + \sum_{j=1}^e b_j h_j$ ($a_i, b_j \in \mathbb{C}$), put $G_K = \sum_{i=1}^d a_i g_i \in S_2(N)$.

Definition 4.3. Let $F(z) \in \mathbb{C}[[q]]$ ($q = e^{2\pi i z}$) be a formal power series as in Definition 3.1. Fix a fundamental domain R in $\mathbb{H}$ for $\Gamma_0(N)$. We say that $F(z)$ is of level N with respect to R if we have

$$(G_K, F(z))_{N,R} := \int_R G_K \cdot \overline{F(z)} dxdy \neq 0 \quad (z = x + iy)$$

for some imaginary quadratic extension $K/\mathbb{Q}$ whose discriminant is relatively prime to N.

Example 4.4. Let us consider the following two cases.

(1) Let $\{F(z)\}_F$ be a set of formal power series of level N with respect to R such that we have $L(F, 1) := -2\pi i \Gamma(1)^{-1} \int_0^{i\infty} F(z) dz = 0$ and let $\{I, J\}_{I,J}$ denote a set of smooth paths in $\mathbb{H}^*$. Assume that two elliptic curves $\{E_i\}_{i=1,2}$ over $\mathbb{Q}$ of conductor N are connected by the topological family $\{E_F(I, J)\}_{F,I,J}$. Then, Mordell-Weil groups of $\{E_i\}_{i=1,2}$ are of rank 1.
(2) On the other hand, let $\mathbb{E}_1$ (resp. $\mathbb{E}_2$) be an elliptic curve over $\mathbb{Q}$ of conductor N (resp. N'). Here, N' denotes a positive integer such that $N' \mid N$ and $N' < N$. Assume that the Mordell-Weil group of $\mathbb{E}_1$ is of rank 1. Then, though it may happen that the Mordell-Weil group of $\mathbb{E}_2$ is also of rank 1, there is not a set of formal power series of level N connecting both elliptic curves.

In fancy language, we can say that the existence of (non-torsion) rational points on elliptic curves is partially governed by the *singular locus* of special fibers in Spec $(\mathbb{Z})$.

Remark 4.5. Let $\{E_i\}_{i=1,2}$ be two elliptic curves over $\mathbb{Q}$ of conductor N whose Mordell-Weil groups are of rank 1. Take rational newforms $\{f_i\}_{i=1,2} \in S_2(N)$ such that we have $L(f_i, s) = L(E_i, s)$. Assume that the strong Birch and Swinnerton-Dyer conjecture holds ([C]). From the equality $L'(f_i, 1) L_{\epsilon_{K_i}}(f_i, 1) = L'(f_i, \mathbf{1}, 1)$, we obtain $L'(f_i, \mathbf{1}, 1) > 0$ and thus $(G_{K_i}, f_i)_{N,R} > 0$. Here, we choose imaginary quadratic fields $K_i/\mathbb{Q}$ such that we have $L_{\epsilon_{K_i}}(f_i, 1) \neq 0$. Define a set of formal power series by

$$F_t(z) = t f_1(z) + (1 - t) f_2(z) \quad (0 \leq t \leq 1).$$

If we can take $K_1 = K_2$ (e.g. two elliptic curves of conductor 91 and $\mathbb{Q}(\sqrt{-3})$ [C, p.118 and 223-224]), we obtain $(G_{K_i}, F_t(z))_{N,R} > 0$ for all $0 \leq t \leq 1$. Thus, though this set of formal power series $\{F_t(z)\}_{0 \leq t \leq 1}$ (regrettably) does not satisfy the compatible conditions in Definition 3.1, two elliptic curves $\{E_i\}_{i=1,2}$ are connected by this set of formal power series *of level* N anyway.

References

[AL] Atkin, A. O. L.; Lehner, J.:*Hecke operators on* $\Gamma_0(m)$. Math. Ann. 185. 1970. 134–160.

[BCDT] Breuil, C.; Conrad, B.; Diamond, F.; Taylor, R.:*On the modularity of elliptic curves over* $\mathbb{Q}$*: wild 3-adic exercises.* J. Amer. Math. Soc. 14 (2001), no. 4, 843–939

[C] Cremona, J.E.: *Algorithms for modular elliptic curves.* Second edition. Cambridge University Press, Cambridge, 1997.

[CW] Coates, J.; Wiles, A.:*On the conjecture of Birch and Swinnerton-Dyer.* Invent. Math. 39 (1977), no. 3, 223–251.

[DS] Diamond, F.; Shurman, J.:*A first course in modular forms.* GTM, 228. Springer-Verlag, New York, 2005.

[GZ] Gross, B.H.; Zagier, D.B.:*Heegner points and derivatives of* L*-series.* Invent. Math. 84 (1986), no. 2, 225–320.

[Kn] Knapp, A.W.:*Elliptic curves.* Mathematical Notes, 40. Princeton University Press, Princeton, NJ, 1992. xvi+427 pp.

[Ko] Kolyvagin, V.A.:*Finiteness of* $E(\mathbb{Q})$ *and* $Y(E,\mathbb{Q})$ *for a subclass of Weil curves.* Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), no. 3, 522–540, 670–671.

[TW] Taylor, R.; Wiles, A.:*Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) 141 (1995), no. 3, 553–572.

[Wa] Waldspurger, J.L.:*Correspondances de Shimura et quaternions.* Forum Math. 3 (1991), no. 3, 219–307.

[Wi] Wiles, A.:*Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) 141 (1995), no. 3, 443–551.

Department of Mathematics, Hokkaido University, Sapporo 060-0810, Japan

E-mail address: morita@math.sci.hokudai.ac.jp